UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/573,684	01/04/2007	Yuichi Futa	2006_0401A	3546

52349 7590 03/15/2010

WENDEROTH, LIND & PONACK L.L.P.
1030 15th Street, N.W.
Suite 400 East
Washington, DC 20005-1503

EXAMINER	
VAUGHAN, MICHAEL R	
ART UNIT	PAPER NUMBER
2431	

NOTIFICATION DATE	DELIVERY MODE
03/15/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ddalecki@wenderoth.com
eoa@wenderoth.com

Office Action Summary	Application No.	Applicant(s)	
	10/573,684	FUTA ET AL.	
	Examiner	Art Unit	
	MICHAEL R. VAUGHAN	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01 February 2010*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *18-39* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *18-20, 22-27,30-38* is/are rejected.

7)☒ Claim(s) *21,28 and 29* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application.
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on **2/1/10** has been entered.

Claims 1, 2, 5, 10-12, and 14-17 have been canceled. Claims 18-39 have been added.

Response to Amendment

Claim Objections

Claims 19-23 and 25-34 are objected to because of the following informalities:

As per claim 19, the preamble states that encrypted communication occurs using a share key. However, no shared key is explicitly created or used in the claim.

As per claims 22 and 23, they are objected for the same reason as claim 19.

As per claim 21, a third key is defined twice. Also, the shared key is defined twice.

As per claim 28, the shared key is defined again.

As per claim 29, both the first and second seed values are named 's'.

Response to Arguments

Applicant's arguments with respect to claims 18, 19, 22, and 23 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 18-20, 25-27, 30-32, and 35-37 are rejected under 35 U.S.C. 103(a) as being unpatentable over USP 5,371,794 to Diffie et al., hereinafter **Diffie** in view of USP 5,953,420 to Matyas Jr. et al., hereinafter **Matyas** and in view of USP 4,918,728 to Matyas Jr. et al., hereinafter **Abraham** (second inventor's name to distinguish prior art).

As per claim 18, Diffie teaches an encrypted communication system comprising:

a first device [base Fig. 4a, 103];

and a second device [mobile; Fig. 4a, 100], wherein said first device includes:

a first data generation unit operable to encrypt a first key using a public key of said second device to generate first encrypted key data, and transmit the first encrypted key data to said second device (col. 7, lines 65-66);

a first decryption unit operable to receive, from said second device, second encrypted key data generated by said second device encrypting a third key using a public key of said first device, and decrypt the second encrypted key data using a private key of said first device to obtain a second key (col. 8, lines 49-53);

a first key generation unit operable to perform a predetermined operation using the first and second keys, generate a part of a result of the predetermined operation as a first encryption key (col. 65-67)

and

a first communication unit operable to encrypt first transmission data using the first encryption key to generate first encrypted data (col. 7, line 7), apply a one-way operation to the first transmission data [CRC; col. 10, lines 5-10]

and transmit the first encrypted data and the first detection value to said second device (col. 10, lines 9-15),

and said second device includes:

a second data generation unit operable to encrypt the third key using the public key of said first device to generate the second encrypted key data, and transmit the second encrypted key data to said first device (col. 8, lines 49-53);

a second decryption unit operable to receive, from said first device, the first encrypted key data generated by said first device encrypting the first key using the public key of said second device, and decrypt the first encrypted key data using a private key of said second device to obtain a fourth key (fig. 5a, and col. 8, lines 44-45);

a second key generation unit operable to perform the predetermined operation using the third and fourth keys, generate a part of a result of the predetermined operation as a second encryption key (col. 8, lines 43-46); and

a second communication unit operable to receive the first encrypted data and the first detection value (col. 7, line 7, and col. 10, lines 5-15), decrypt the first encrypted data using the second encryption key to generate second transmission data [inherently what the session key is used for], apply a one-way operation to the second transmission data calculate a second detection value [checks the check sum value], compare the first and second detection values, and when the first and second detection values match, recognize the second transmission data as valid, and when the first and second detection values do not match, recognize the second transmission data as invalid (col. 10, lines 12).

Diffie teaches generating a session key by XOR'ing two random keys. Diffie does not teach that the XOR operation yields more than one key. Matyas teaches two keys can be concatenated together and then hashed to achieve a result. The result

yields a plurality of keys (fig. 2, and col. 5, lines 60-64). These keys, generated by both sides of the communication can then be used to secure data transmission. Matyas' method of generating multiple keys can be seen as more efficient than the key change as taught by Diffie (col. 10, lines 25-40). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to substitute Matyas' method of generating the many keys needed for securing data transmissions.

Diffie is silent in explicitly teaching the use of a message authentication codes which use a hash key. However the use of MACs is notoriously well known in the art. They are known to provide tamper detection in data packets by creating a hash of the message with the aid of a hash key. Abraham teaches the method of using a hash key with a MAC function to apply a one-way operation [the hash] to transmission data to calculated a first detection value [result of the MAC] to be used by the receiver to detect tampering of the data packet (col. 43, lines 60-68). It is also well known in the art, how the receiver uses the received MAC, to verify the data. As taught by Abraham, the receiver has its own sets of keys, uses the same hash key used by the sender to hash the received message and compare its calculated value to the received MAC. MACs are used to detect tampering and are more secure than check sums. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to substitute the check sums for MACs because they provide a greater level of security. MACs simply use encryption keys. Therefore, any of the keys generated by the concatenation and subsequent hash could have been used as a hash key. As long as both sides pick the same key, tampering can be detected. Matyas teaches a system in

which both sides can use keys synchronously. There the result of using hash keys as taught by Abraham would have been predictable.

As per claim 19, it is rejected for the same reasons as claim 18.

As per claim 20, Diffie teaches said key generation unit determines the result of the predetermined operation by performing, as the predetermined operation, an exclusive OR operation using the first and second keys (col. 8, line 47).

As per claims 22 and 23, they are rejected for the same reasons as claim 18.

As per claims 24-27, 30, and 35, Diffie is silent in explicitly teaching the first encryption key and the first hash key are included in a hash calculation result that is generated by performing a hash calculation using the concatenated data generated by concatenating the first and second keys. This limitation was shown to be taught by Matyas (col. 5, lines 60-65) in the rejection of claim 18. Examiner supplies the same rationale in rendering these claims obvious as recited in the rejection of claim 18.

As per claims 31 and 36, they are rejected for the same reasons as recited in the rejection of claim 18. Claims 31 and 36 only show the original sending device in the role of receiving encrypted data from the original receiver device and it carrying out the same tamper detection process that the original receiver performed. It is obvious that

both sides of the communication send/receive and use the tamper detection values [MAC].

As per claims 32 and 37, Diffie teaches an authentication unit operable to authenticate the other device, using the first encryption key (col. 9, line 15).

Claims 33, 34, 38, and 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Diffie, Matyas, and Abraham as applied to claims 18 and 19 above, and further in view of USP Application Publication 20030041253 to Matsui et al., hereinafter Matsui.

As per claims 33 and 38, Diffie, Matyas, and Abraham are silent in explicitly teaching the authentication unit (i) generates a first authentication value, encrypts the first authentication value using the first encryption key to generate a first encrypted value, and transmits the first encrypted value to the other device, and (ii) receives, from the other device, a second authentication value generated by decrypting the first encrypted value using a second encryption key held by the other device, and judges whether the first and second authentication values match, and said communication unit performs communication with the other device when the authentication values are judged to match. Examiner recognizes these steps as an authentication challenge/response, known in the art of cryptography. Matsui explicitly teaches this well-known procedure (0054) whereby the sender challenges the receiver to prove it

possesses knowledge of a shared key, thereby authenticating the receiver. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to implement this authentication procedure within the combined system of Diffie, Matyas, and Abraham, because it adds another level of security. Namely, security is increased by adding the step of authentication by proving the receiver was able to correctly generate the session key. Diffie already teaches mutual authentication and this is simply another equivalent and known way of doing so.

As per claims 34 and 39, Diffie, Matyas, and Abraham fail to teach the authentication unit receives, from the other device, a third encrypted value generated by encrypting a third authentication value using the second encryption key held by the other device,

decrypts the third encrypted value using the first encryption key to obtain a fourth authentication value, and transmits the fourth authentication value to the other device, and said communication unit performs the communication when the other device judges the third and fourth authentication values to match. Examiner recognizes these limitations as the other side of the mutual authentication initiated by the original receiver side. The process is the same as that of claims 33 and 38. It is just from the original sender's point of view in proving itself to the original receiver. Thus, the other half of the mutual authentication is now claimed. Therefore, Examiner supplies the same rationale as recited in the rejection of claims 33 and 38 because the process is the same.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL R. VAUGHAN whose telephone number is (571)270-7316. The examiner can normally be reached on Monday - Thursday, 7:30am - 5:00pm, EST. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William Korzuch can be reached on 571-272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/M. R. V./

Examiner, Art Unit 2431

/William R. Korzuch/

Supervisory Patent Examiner, Art Unit 2431